オフィス宅ふぁいる便®

シングルサインオン
設定マニュアル
（Azure AD 編）

Ver. 1.0.0

株式会社オージス総研

目次

1. はじめに 3
1.1. 機能概要 3
1.2. 要件 3
1.3. 本書の目的 3
1.4. ご注意 4
2. 設定手順 5
2.1. 利用開始までの流れ 5
2.2. 各種設定 5
(1) エンタープライズアプリケーションの新規作成 5
(2) サービスプロバイダ側のメタデータのアップロード 6
(3) ユーザー属性とクレームの設定 7
(4) シングルサインオンを行うユーザーグループの設定 9
2.3. メタデータの取得 10
付録. 改訂履歴 12

1. はじめに

1.1. 機能概要

シングルサインオンとは、オフィス宅ふぁいる便（以下「当サービス」という。）にログインする際、サイトに登録されたパスワードを利用せず、ID プロバイダ（以下「IdP」という。）と呼ばれる外部の認証サービスを利用したユーザ認証を可能にする機能です。
当サービスでは、エンタープライズプランおよびプロフェッショナルプランでご契約いただいたお客様を対象に、機能を提供しております。なお、デフォルトでは有効になっていません。

1.2. 要件

機能を利用するには、以下の条件を満たしている必要があります。

項目	内容
契約プラン	以下のうち、いずれかであること。 ● エンタープライズプラン ● プロフェッショナルプラン ※スタンダードプランのお客様はご利用いただけません。
プロトコル	IdP 側が SAML 認証を連携できる機能を有していること。
NameIDFormat 形式	以下の形式に対応していること。 urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified （参考）unspecified である理由として、当サービスではメールアドレスを一意ではなく、重複してアカウント情報として登録することが可能であるためです。
POST バインド方式	HTTP POST バインド方式に対応していること。 ※HTTP リダイレクト方式、HTTP アーティファクト方式には対応していません。
アカウント登録	事前にサイトにアカウント登録されていること。IdP 側に、サイトのログイン ID と一致するユーザ情報が登録されていること。

1.3. 本書の目的

本書は、Microsoft 社の Azure Active Directory（以下、「Azure AD」という。）をご利用のお客様を対象に、当サービスにてシングルサインオン機能をご利用いただく際の、Azure AD 側の設定手順について理解していただくことを目的としています。

1.4. 本書に関するご注意

著作権について

- 本書の著作権は株式会社オージス総研（以下「弊社」という。）に帰属します。
- 本書の内容、テキスト、画像などの無断転載を禁じます。

商標について

- 「オフィス宅ふぁいる便」、「オフィス宅ふぁいる便」ロゴは、弊社の商標または登録商標です。
- その他、本書に記載されている会社名、製品名は、各社の商標または登録商標です。
- 本書に記載されている会社名、製品名等には必ずしも商標表示（TM ・R）を付記しておりません。

その他

- 本書は、予告なしに変更されることがあります。
- 例示として記載された氏名やメールアドレス、ドメイン、IP アドレスはすべて架空のものです。

2. 設定手順

2.1. 利用開始までの流れ

利用するには、以下の設定が必要です。

① 当サービスの管理画面にて、サービスプロバイダ（当サービス）側のメタデータを取得する。（メニュー[システム設定]＞[シングルサインオン]）

② IdP（Azure AD）側の各種設定を行う。 →本書「2.2. 各種設定」

③ IdP 側のメタデータを取得する。 →本書「2.3 メタデータの取得」

④ 当サービスの管理画面にて、IdP 側のメタデータを登録する。（メニュー[システム設定]＞[シングルサインオン]）

⑤ 当サービスの管理画面にて、機能を有効化する。（メニュー[システム設定]＞[パラメータ]）

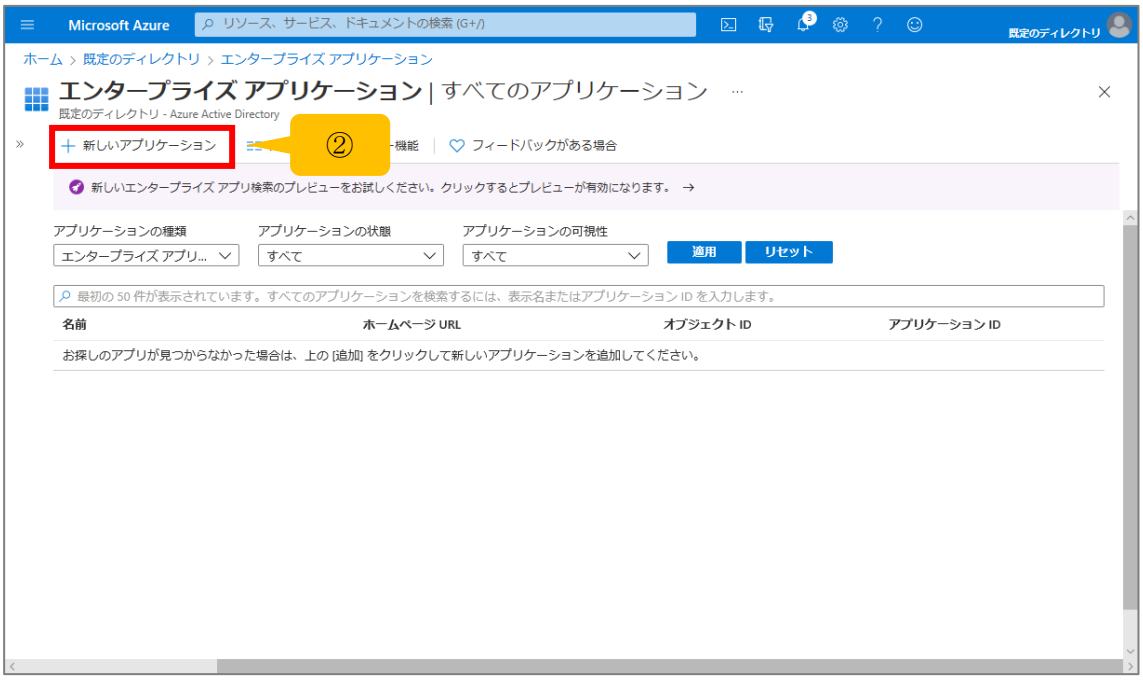
このうち、①、④、⑤の操作手順については、別紙『管理者向け 操作・運用マニュアル』をご参照ください。（該当箇所は「5.3. シングルサインオン」です。）本書では、②、③の IdP 側の操作手順について説明します。

2.2. 各種設定

(1) エンタープライズアプリケーションの新規作成

① Azure AD のコンソールにて「エンタープライズアプリケーション」を選択する。

② 「＋新しいアプリケーション」をクリックする。



③ 「＋独自のアプリケーションの作成」をクリックする。

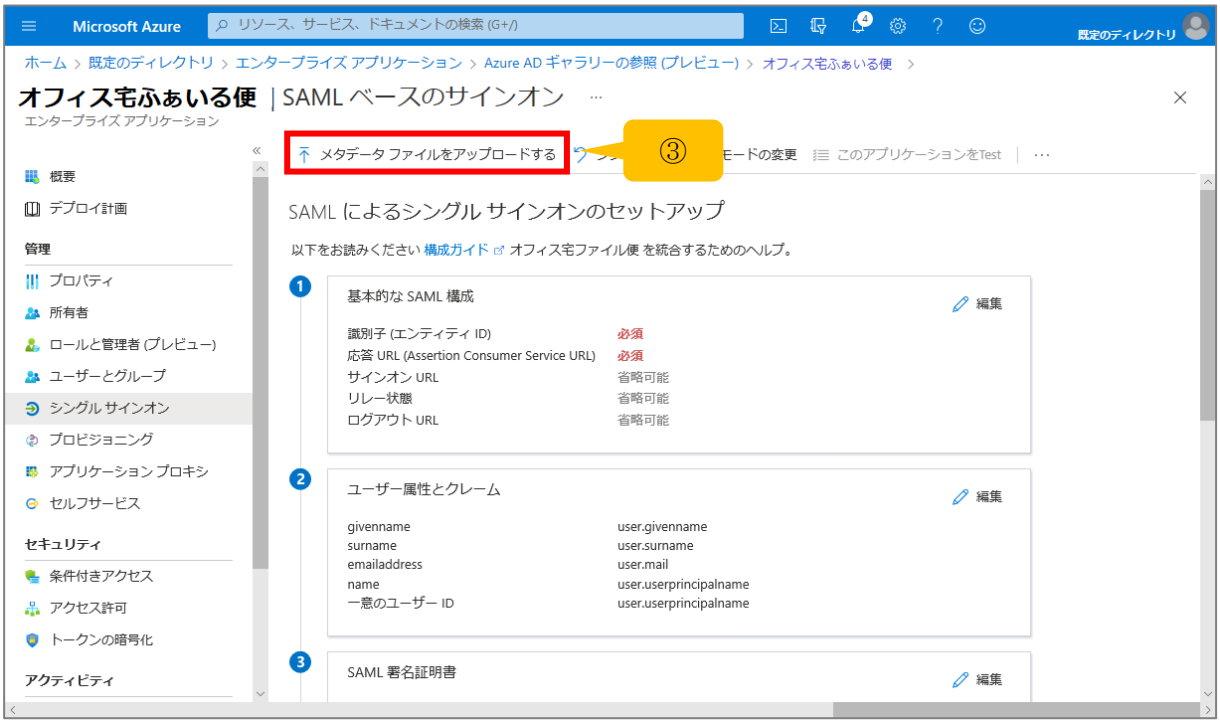
④ 画面右に「独自のアプリケーションの作成」の画面が開かれたら、アプリケーションの名前に「オフィス宅ふぁいる便」を入力し「作成」をクリックする。

(2) サービスプロバイダ側のメタデータのアップロード

① 「２．シングル サインオンの設定」をクリックする。

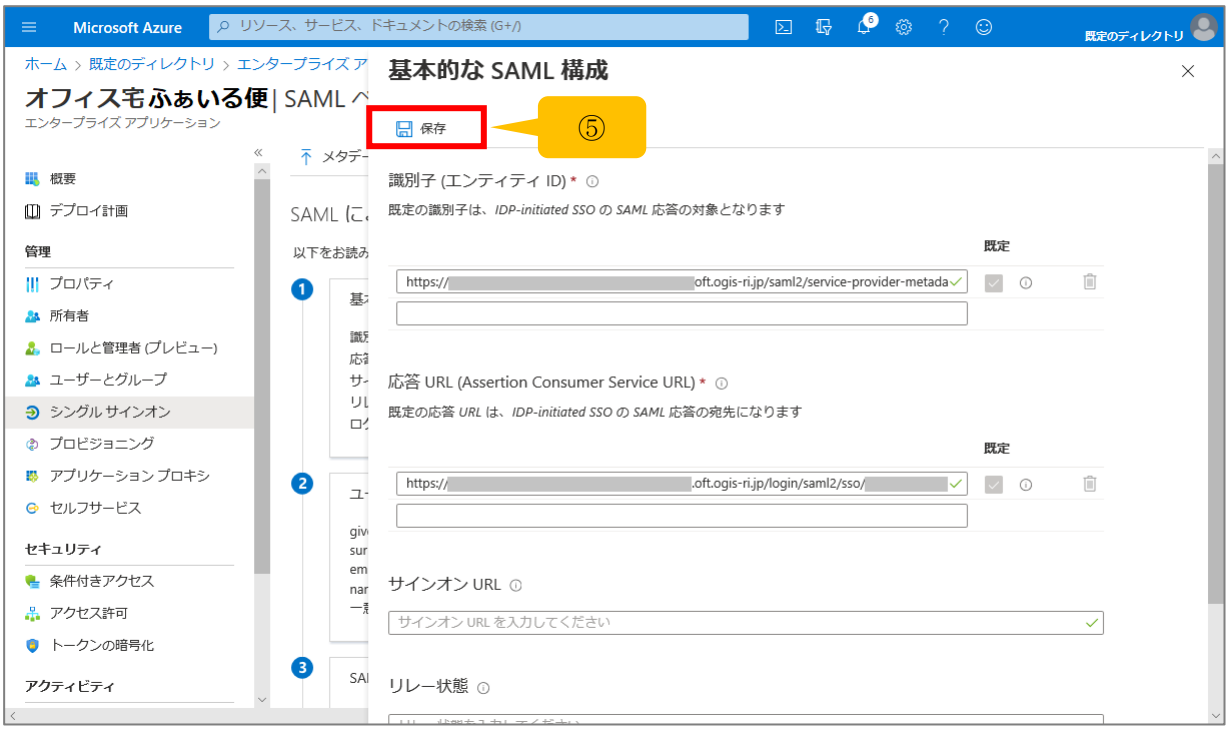
② 「SAML」をクリックする。

③ 「メタデータファイルをアップロードする」をクリックする。



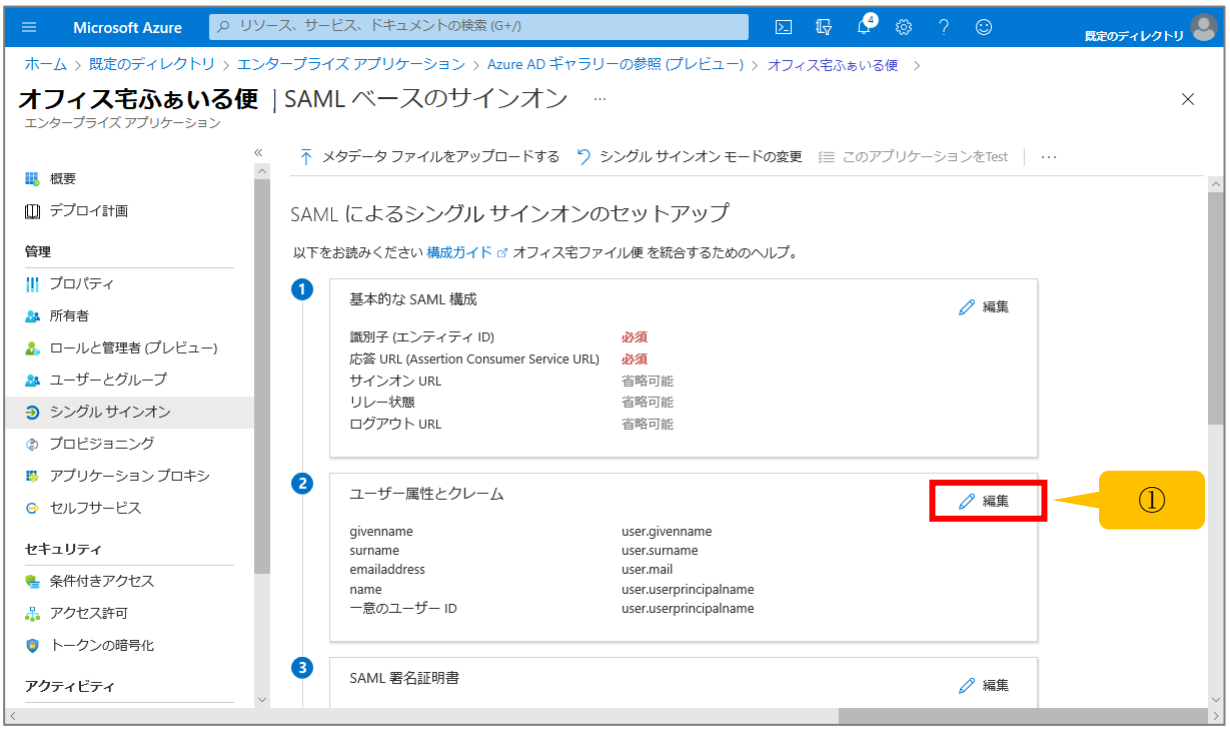
④ あらかじめ取得しておいた、当サービス側のメタデータファイルを選択し、「追加」をクリックする。

⑤ 画面右に「基本的な SAML 構成」の画面が開かれたら、「保存」をクリック。



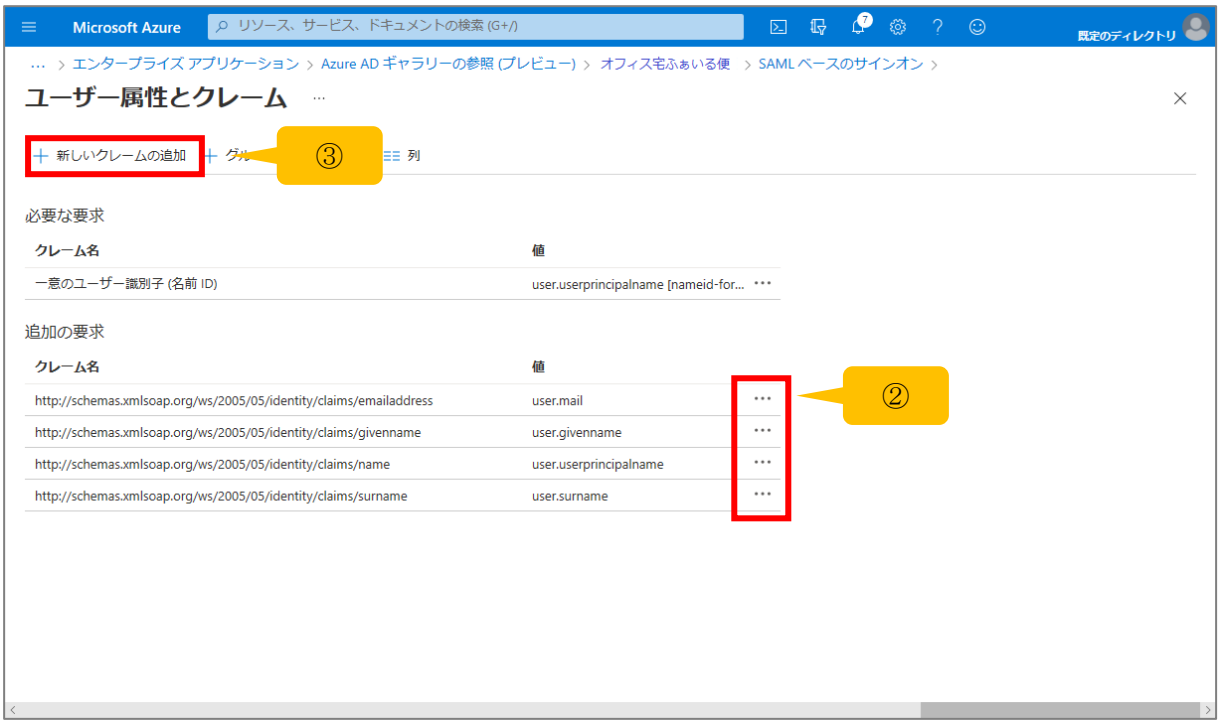
(3) ユーザー属性とクレームの設定

① 「ユーザー属性とクレーム」の「編集」をクリックする。

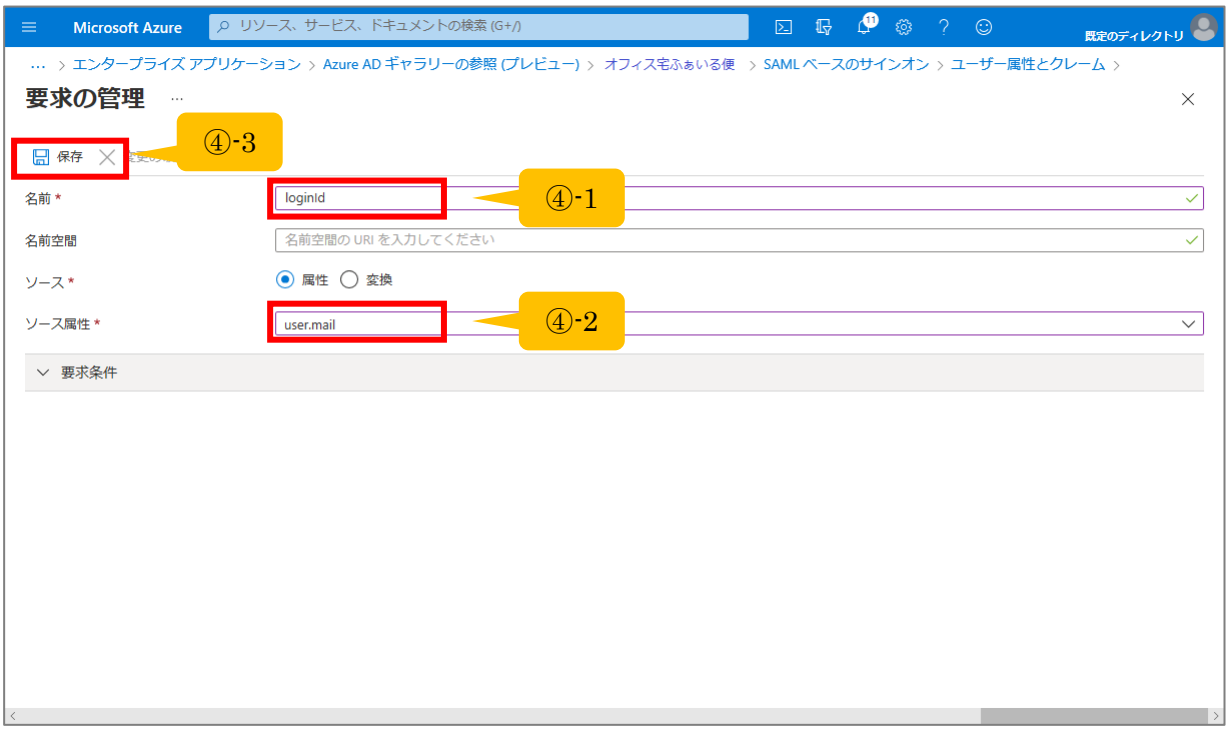


② 初期状態で設定されいてる 4 つの追加の要求の項目について、右端「…」をクリックして削除する。

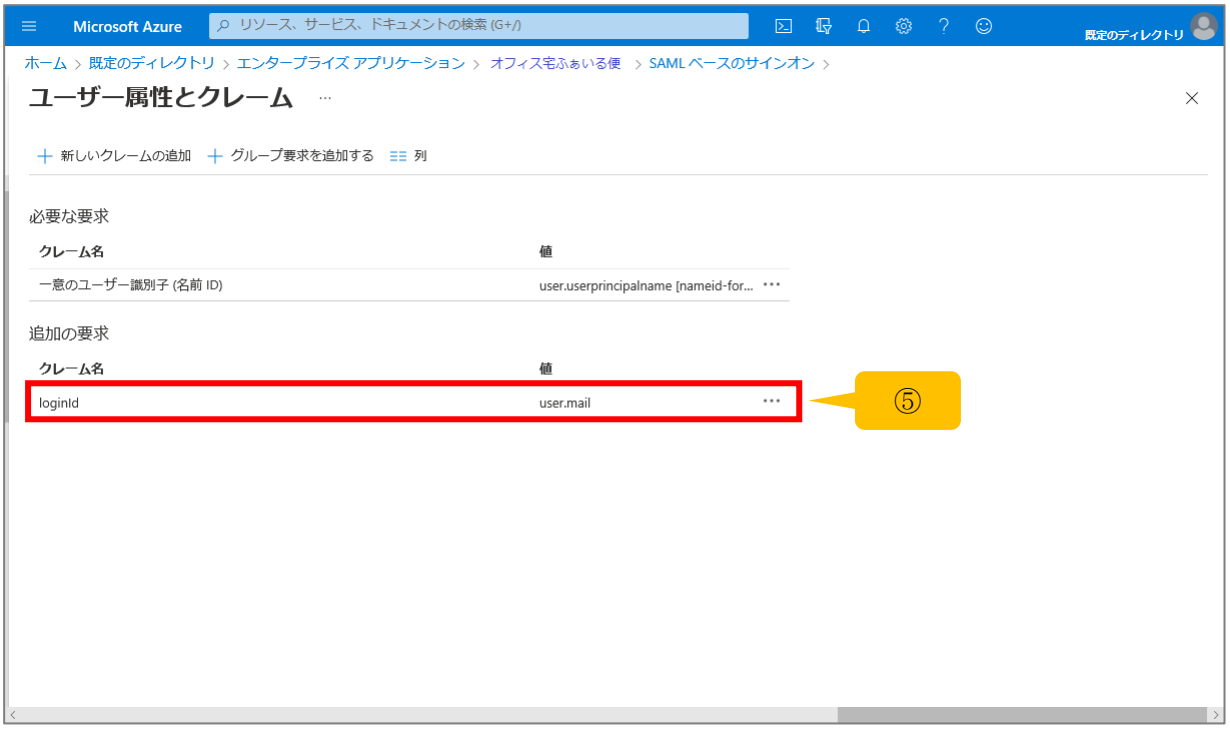
③ 「新しいクレームの追加」をクリックする。



④ 「名前」に「loginId」と入力し、「名前空間」は空欄のまま、「ソース」はデフォルトの「属性」のまま、「ソース属性」は当サービスのログイン ID と一致するデータを入力したら、「保存」をクリックする。

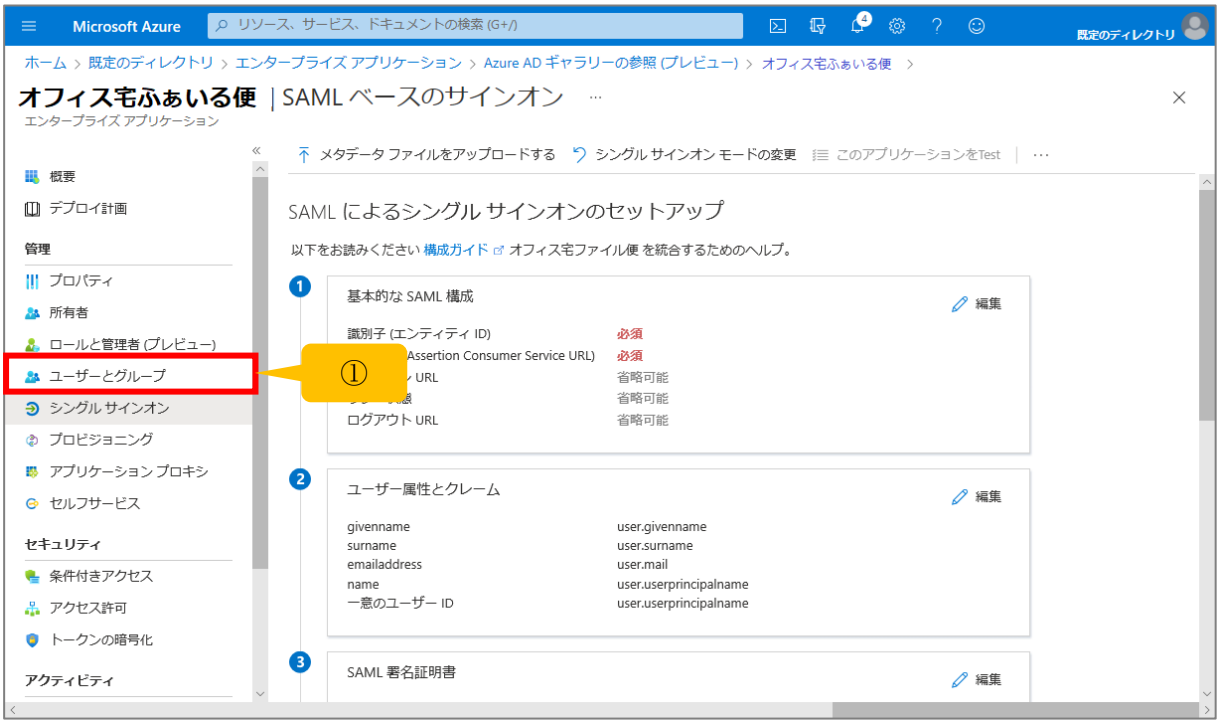


⑤ クレーム名は初期設定のまま、追加の要求に「loginId」のみ設定されていることを確認する。

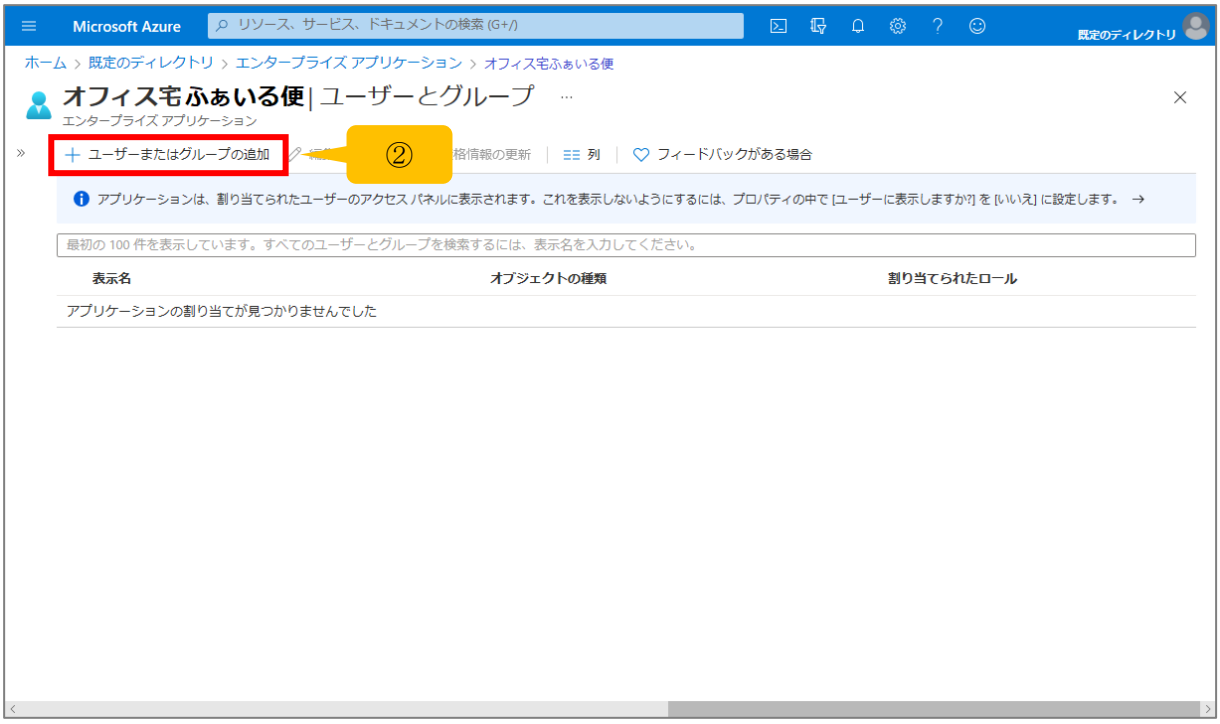


(4) シングルサインオンを行うユーザーグループの設定

① 画面左のメニューから「ユーザーとグループ」をクリックする。



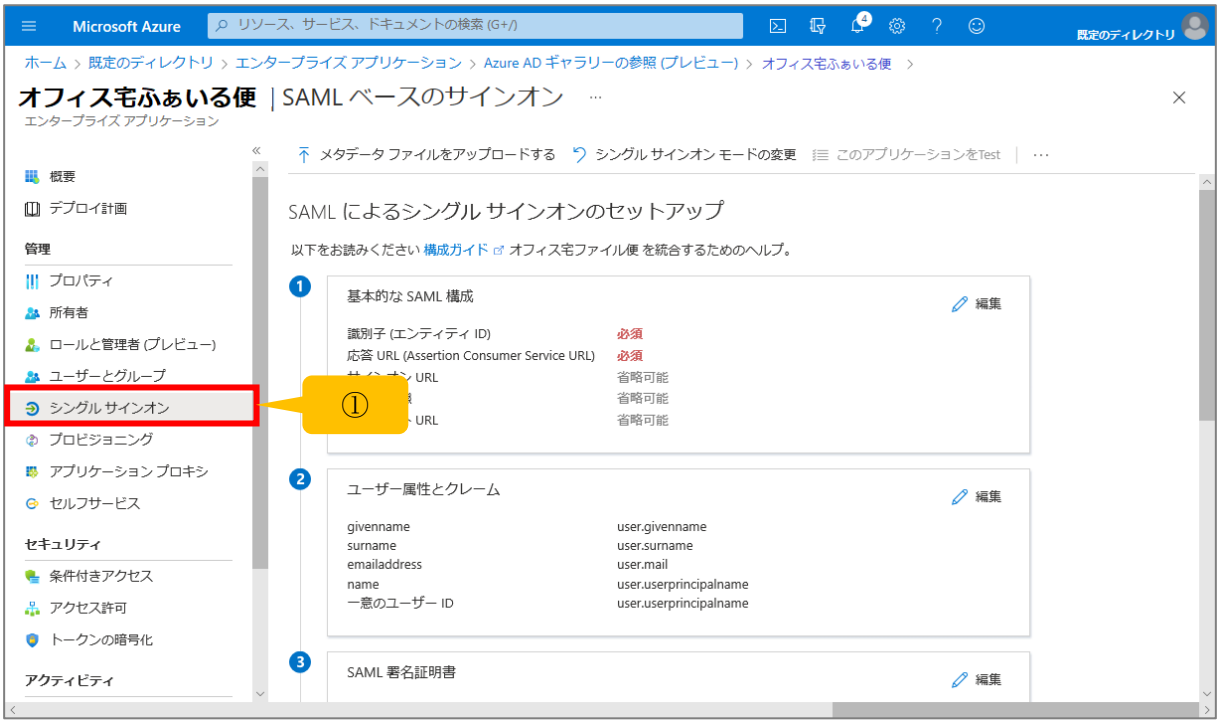
② 「＋ユーザーまたはグループの追加」をクリックする。



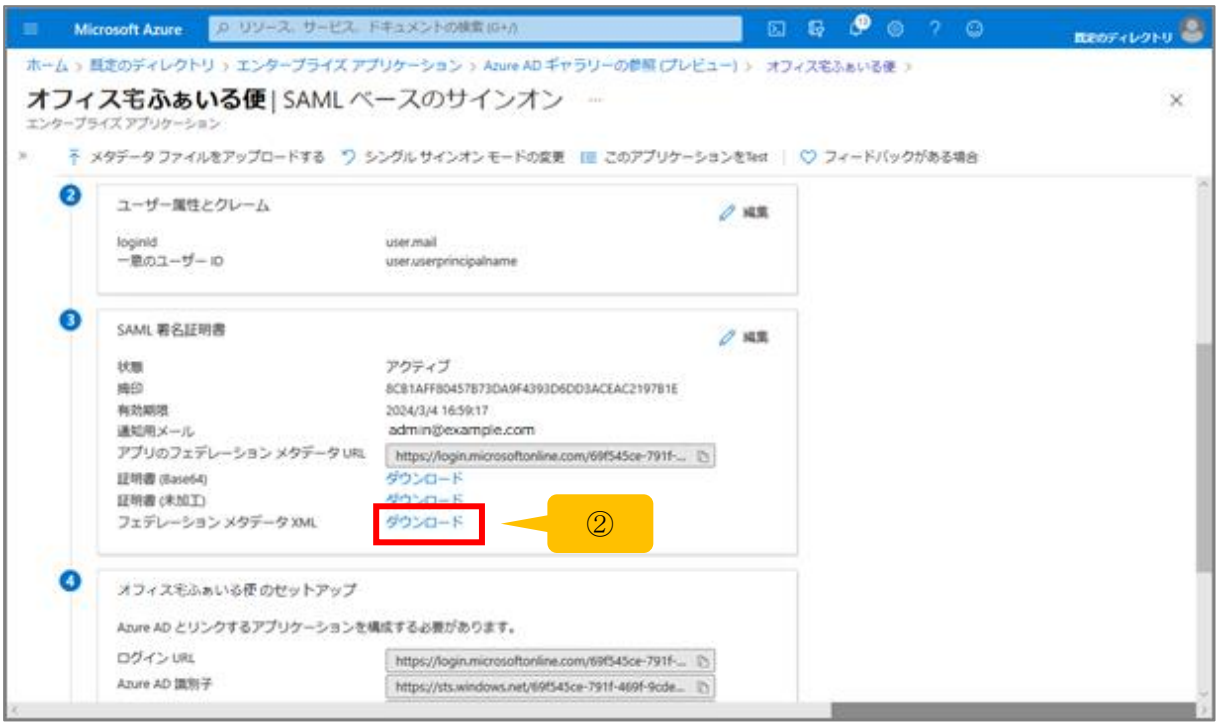
③ 当サービスでシングルサインオンを行うユーザーまたはロールを選択する。

2.3. メタデータの取得

① 画面左のメニューから「シングルサインオン」をクリックし、SAML ベースのサインオン画面へ戻る。



② フェデレーションメタデータ XML の「ダウンロード」をクリックする。ファイルを任意のパスに保存する。



Azure AD 側での操作は以上です。
このあとは、当サービスの管理画面にて設定を行ってください。

付録. 改訂履歴

日付	版数	変更内容
2022/5/27	1.0.0	初版作成